NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Boiler malfunction forces residents to evacuate. A water main break backed up a boiler and led to the flooding and evacuation of an 18-unit apartment building in Moorhead. More than two dozen residents were offered assistance by the American Red Cross, who provided temporary living accommodations at the Minnesota State University Moorhead campus. Source: http://www.valleynewslive.com/story/21778565/boiler-malfunction-forcesresidents-to-evacuate

Regional

(Minnesota) **Tax scam allegedly run from Minnesota prison.** The IRS and other authorities are investigating a tax refund fraud scheme allegedly run by Minnesota prison inmates and their not-incarcerated accomplices. The investigation involves hundreds of falsified tax returns from between 2006 and 2012. Source: http://www.startribune.com/local/199958841.html

(Minnesota) **$15,000 in stolen copper wire is recovered.** Police in St. Cloud recovered stolen copper wiring worth close to $15,000 during a patrol stop. The bulk of the wiring was reported stolen weeks ago from a construction site. Source: http://www.sctimes.com/article/20130322/NEWS01/303220019/-15-000-stolen-copper-wire-recovered?nclick_check=1

(Montana) **Fort Peck Dam repairs to cost $42.9 million after damage from record 2011 flooding.** The U.S. Army Corps of Engineers approved spending a part of $234 million slated for 100 projects along the Missouri River on the Fort Peck Dam. Six contracts were awarded to spend the $42.9 million allocated to the project, including a $33.8 million contract to rehabilitate the dam's plunge pool. Source: http://www.therepublic.com/view/story/2841af2d6c7b4abfa08a0d4a64092dcc/MT--Fort-Peck-Dam

National

Nothing Significant to Report

International

South Korea data-wipe malware spread by patching system. South Korean antivirus firm AhnLab stated that the malware that spread through banking and communications Web sites in that country was distributed via compromised patch management systems and delivered to targets as if it were a legitimate software update. Source: http://www.theregister.co.uk/2013/03/25/sk_data_wiping_malware_latest/

Banking and Finance Industry

Bitcoin exchange faces DDoS, even as the digital currency surges. Mt. Gox, an exchange for the virtual currency Bitcoin, was affected by a distributed denial of service (DDoS) attack March 28. Payment company Dwolla, which also deals in Bitcoins, was also subject to DDoS attacks March 27. Source: http://www.computerworld.com/s/article/9237979/Bitcoin_exchange_faces_DDoS_even_as_the_digital_currency_surges

Wells Fargo warns of ongoing DDOS attacks. Wells Fargo stated that their Web site was coming under distributed denial of service (DDoS) attacks March 26, but that most customers were not affected. Source: http://www.cso.com.au/article/457405/wells_fargo_warns_ongoing_ddos_attacks/

U.S. charges two in $27 million insider-trading scheme. A former Foundry Networks executive and a hedge fund analyst were charged in federal court for allegedly trading on insider information and netting $27 million in illicit gains. Source: http://www.bloomberg.com/news/2013-03-26/u-s-charges-two-in-27-million-insider-trading-scheme.html

"Dump Memory Grabber" malware steals data from ATMS and POS systems. Researchers from Group-IB identified malware dubbed "Dump Memory Grabber" that can infect point of sale (PoS) devices and ATMs, steal customer account information, and send the information to a remote server. The malware has already taken information from some U.S. bank customers. Source: http://news.softpedia.com/news/Dump-Memory-Grabber-Malware-Steals-Card-Data-from-ATMs-and-POS-Systems-340758.shtml

VSkimmer trojan steals card data on point-of-sale systems. A new trojan called VSkimmer is capable of infecting Windows systems and stealing financial information from any point of sale (PoS) devices attached to infected systems. VSkimmer appears to be similar to the Dexter PoS malware and to spread via USB devices. Source: http://www.scmagazine.com/vskimmer-trojan-steals-card-data-on-point-of-sale-systems/article/285725/

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Nothing Significant to Report

Communications Sector

Nothing Significant to Report

Critical Manufacturing

Honda recall 183,000 vehicles due to brake malfunctions. Honda announced it will recall a total of 183,000 model year 2005 Honda Pilot, Acura MDX, Acura RL vehicles and 800 model year 2006 Acura MDX vehicles due to a problem with their vehicle stability assist (VSA) systems that could cause unexpected braking. Source: http://charlottesville.legalexaminer.com/defective-and-dangerous-products/honda-recalls-183000-vehicles-due-to-brake-manfunctions.aspx?googleid=307712

Honda recalling 76,000 Acura TSX vehicles from 2004 to 2008. Honda announced a recall of 76,253 Acura TSX vehicles sold in or currently located in cold weather States due to road salt potentially corroding the vehicles' electronic control units (ECU), creating the potential for stalling. Source: http://www.examiner.com/article/honda-recalling-76-000-acura-tsx-vehicles-from-2004-to-2008

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

IRS expands ID theft refund access for police. The U.S. Internal Revenue Service announced it will expand nationwide a pilot program that gives law enforcement access to federal data on tax returns to help fraud and identity theft investigations. The program expansion goes into effect starting March 29. Source: http://www.bizjournals.com/southflorida/blog/2013/03/irs-expands-tax-refund-data-access-for.html

(Missouri) **Man allegedly poses as cop to rape woman, police fear more victims.** Kansas City police arrested and charged a man with impersonating a police officer in order to sexually assault a woman. The man pulled over a cab and indicated he was a cop, he then took the woman into his truck and threatened to take her to jail if she did not have relations with him, assaulting her when she refused. Source: http://www.kpho.com/story/21761304/man-posing-as-police-officer-rapes

Energy

Nothing Significant to Report

Food and Agriculture

Outbreak of E.coli O121 Linked to Frozen Snack Products. Rich Products Corporation of Buffalo, NY issued a voluntary recall on a variety of frozen snack products that have been connected to an outbreak of E. coli O121 that has sickened at least 24 people in 15 states.

Source: http://www.foodsafetynews.com/2013/03/mini-snack-products-recalled-for-e-coli-risk/#.UVV82xykrMg

FDA adds lionfish to list of fish that may carry ciguatoxins. The U.S. Food and Drug Administration created draft guidance for the fish processing industry listing the types of fish that have been found to harbor ciguatoxins, and recently included two species of lionfish that had not previously been named as a potential ciguatera fish poisoning threat. Source: http://www.foodsafetynews.com/2013/03/fda-adds-lionfish-to-list-of-fish-that-may-carry-ciguatoxins/#.UVLZ6BykrMg

Government Sector (including Schools and Universities)

Sykipot cybercriminals use new exploits to target government organizations. Cybercriminals have improved their Sykipot campaign targeting the defense industry and government organizations by setting up fake Web sites that appear to be legitimate government organizations and leading users through malicious links. Source: http://news.softpedia.com/news/Sykipot-Cybercriminals-Use-New-Exploits-to-Target-Government-Organizatons-339540.shtml

Information Technology and Telecommunications

Zeus still king of the botnets, say researchers. Researchers at McAfee found that the Zeus malware continues to be the most popular botnet family, with its variants accounting for 57.9 percent of botnet malware infections. Source: http://www.v3.co.uk/v3-uk/news/2258398/zeus-still-king-of-the-botnets-say-researchers

Largest-ever DDoS campaign demonstrates danger of new attack method. A massive distributed denial of service (DDoS) campaign targeting anti-spam organization Spamhaus reached 300 GB per second, illustrating how use of open recursive resolvers can amplify the power of DDoS attacks. Source: http://www.eweek.com/security/largest-ever-ddos-campaign-demonstrates-danger-of-new-attack-method/

Dirty smartphones: Devices keep traces of files sent to the cloud. University of Glasgow researchers found that remnants of files uploaded to cloud services from smartphones are left on the devices, potentially allowing hackers to access the files or gain access to cloud services. Source: http://www.networkworld.com/news/2013/032613-dirty-smartphones-268114.html

Honeypot stings attackers with counterattacks. A researcher outlined in a paper how he set up a „honeypot" to catch attackers and enabled the honeypot to install a backdoor agent on attackers" computers via a Java applet as a research experiment, revealing information on them. Source: http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240151740/honeypot-stings-attackers-with-counterattacks.html

U.S. and Russia --not China-- lead list of malicious hosting providers. According to Host Exploit‟s quarterly World Hosts Report, the U.S. and Russia ranked as the countries with the highest number of malicious hosting providers. Source: http://threatpost.com/en_us/blogs/us-and-russia-not-china-lead-list-malicious-hosting-providers-032713

Attackers shifting to delivering unknown malware via FTP and Web pages. A report by Palo Alto Networks found that malware that goes undetected by antivirus programs has shifted primarily to Web-based exploits rather than email-based exploits, with 94 percent coming from Web browsing or Web proxies. Source: http://threatpost.com/en_us/blogs/new-report-confronts-unknown-malware-problem-032613

Hackers steal photos, turn wi-fi cameras into remote surveillance device. Researchers from ERNW demonstrated various methods to remotely steal photos, turn cameras on, and execute denial of service (DoS) attacks against Wi-Fi-enabled Canon EOS-1D X cameras. Source: http://www.networkworld.com/community/node/82716

Lime Pop emerges as the latest strain of Android Enesoluty malware. Symantec identified a new variant of the Android. Enesoluty data-stealing malware, spread through an app called Lime Pop. The group behind Enesoluty has been active since summer 2012 and has registered more than 100 domains to host the malicious apps. Source: http://threatpost.com/en_us/blogs/lime-pop-emerges-latest-strain-androidenesouty-malware-032513

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

(Oklahoma) **HIV test urged for 7,000 Oklahoma dental patients.** A Tulsa-based dentist possibly performed practices that could have exposed patients to infectious materials including hepatitis B, hepatitis C, and HIV. Approximately 7,000 patients are being notified by the Tulsa Health Department and the Oklahoma Department of Health about potential exposure to blood borne viruses. Source: http://www.newsnet5.com/dpp/news/national/hiv-test-urged-for-7000-oklahoma-dental-patients

(Texas) **Missing virus vial raises concerns at UTMB facility.** Officials at the University of Texas Medical Branch are searching for a missing vial containing less than a quarter of a teaspoon of the Guanarito virus. The vial was discovered missing during a routine internal inspection and lab

officials believe there was no breach or wrongdoing involved. Source: http://www.chron.com/news/houston-texas/houston/article/Missing-virus-vialraises-concerns-at-UTMB-4380346.php

US authorities indict 44 for role in healthcare fraud scheme. Forty four individuals were indicted in a health care fraud scheme for allegedly helping bribe physicians and medical professionals in exchange for prescriptions for patients with private insurance, Medicaid, and Medicare. Pharmacies along with healthcare agency owners were aiding by facilitating the submissions to fake claims to the insurers. Source: http://news.softpedia.com/news/US-Authorities-Indict-44-People-for-Role-in-Healthcare-Fraud-Scheme-339887.shtml

Transportation

Nothing Significant to Report

Water and Dams

EPA survey finds more than half of the nation's river and stream miles in poor condition. The U.S. Environmental Protection Agency released the results of a comprehensive study of the health of the country's streams and other water sources critical to feeding large bodies of water. The survey's results indicate 55% of the streams and river miles across the country are in poor condition for aquatic life due to excessive levels of harmful elements (nitrogen, phosphorous, mercury) and bacteria, along with increased human disturbance. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/26A31559BB37A7D285257B3A00589DDF

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168